(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33759 A1

(51) International Patent Classification[7]: H04K 1/00, G06F 11/00, 13/36, H04L 9/32

(21) International Application Number: PCT/US00/41797

(22) International Filing Date: 2 November 2000 (02.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/163,231 3 November 1999 (03.11.1999) US

(71) Applicant: AVANTCOM NETWORK, INC. [US/US]; Suite 110, 911 Bern Court, San Jose, CA 95112 (US).

(72) Inventor: PATANKAR, Subhash; 892 Meander Drive, Walnut Creek, CA 94598 (US).

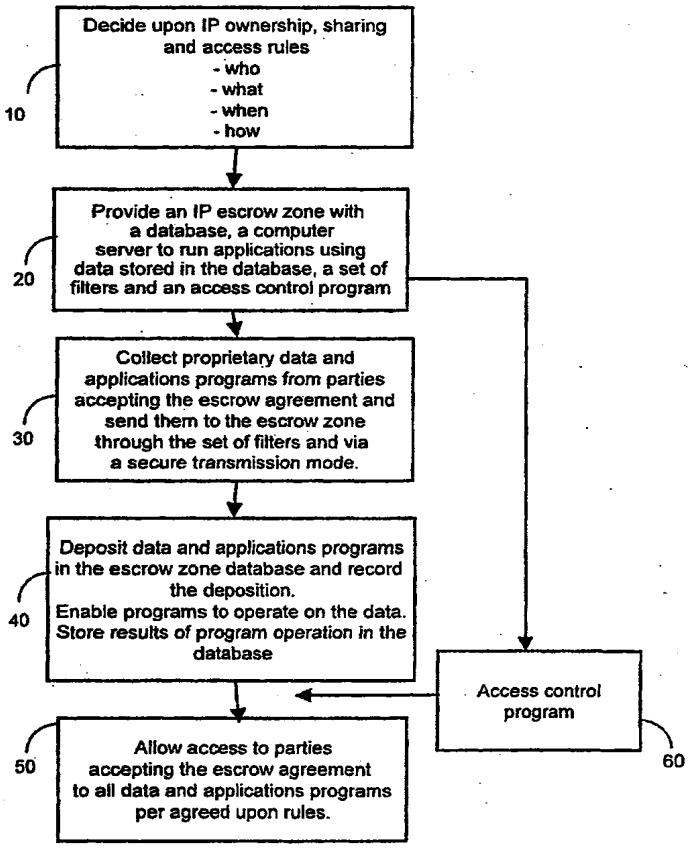
(74) Agent: MEIER, Lawrence, H.; Downs Rachlin & Martin PLLC, 199 Main Street, P.O. Box 190, Burlington, VT 05402-0190 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: METHOD OF SHARING PROPRIETARY INFORMATION



(57) Abstract: A method of sharing proprietary data between two companies includes establishing rules of sharing (10) and providing a secure escrow zone (20) for collecting and distributing the proprietary data. The escrow zone is managed by a third party and includes a database and an access control program for implementing the agreed upon established rules. Data from each of the two companies are selected by passing them through corresponding data filter. The filtered data are then transmitted to the database via a secure transmission mode (30) and are deposited in the database (40). Access to the escrow zone and the database is controlled by the access control program according to the prearranged rules (50). A user can access the escrow zone and the deposited filtered data remotely via an internet network.

WO 01/33759 A1

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BNSDOCID: <WO_____0133759A1_I_>

METHOD OF SHARING PROPRIETARY INFORMATION

Cross Reference to Related Co-Pending Applications

This application claims the benefit of U.S. provisional application Ser. No. 60/163,231 filed on November 3, 1999 and entitled "METHOD AND APPARATUS FOR PROPRIETARY DATA COLLECTION AND DISTRIBUTION" which is commonly assigned and the contents of which are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a method of sharing proprietary information, and more particularly to a method of sharing proprietary information that allows protection of intellectual assets while providing a collaborative working platform.

Background of the Invention

Protection of intellectual property assets is critical for maintaining a competitive advantage in today's business environment. At the same time, today's businesses utilize manufacturing processes, business methods and equipment that are complex. This complexity of modern manufacturing processes, business methods and production equipment has lead to outsourcing of specific tasks and redistribution of responsibilities. This is especially the case for the operation and maintenance of complex production equipment.

In a modern semiconductor fabrication facility (fab), production equipment may be operated, maintained and repaired by different groups of people. These different groups of people often belong to different companies. For example, a particular equipment may be operated by one group of fab employees, serviced by technicians from the original supplier of the equipment and routinely maintained by a third company under contract to the fab. Further, such arrangements may vary from equipment to equipment. In house fab technicians may be fully responsible for some equipment and prohibited from working on others. In some cases they may be permitted to perform certain levels of service before calling in a technician from another company.

In light of this multi-organizational support needed to keep production facilities operating at peak efficiency, manufacturers often have to share information about specific production equipment and manufacturing processes with various organizations. This information is

PNSDOCID: <WO 0133759A1 | >

usually proprietary and is held internally as part of the company's intellectual property assets. Therefore, there is a need for sharing selective equipment and process information while protecting and maintaining ownership of the company's intellectual property assets.

Typically a manufacturer selects the type of data to be collected and the format in which it is stored. Data associated with the manufacturing process parameters, quality control and throughput are usually considered proprietary information and are stored at a server located at the manufacturer's site. Access to the server and to the particular proprietary information is usually limited to certain members of the manufacturer's operation. However, frequently, these data need to be analyzed to determine causes for defects or problems in the manufacturing process and to develop improvements of the process. Expert scientist and specialist from third party organizations are often contracted to conduct this analysis and recommend solutions. In cases where performance of a piece of equipment or consumable material used in the manufacturing process is an issue, suppliers of the specific piece of equipment or material need to be involved. Therefore, there is a need for these outside contracted experts and suppliers to gain controlled access to proprietary data associated with the manufacturing process, in order to work collaboratively with the manufacturer's personnel to solve the problem.

In some cases, equipment suppliers and third party experts have proprietary data and logic embodied in proprietary software application programs, which they do not wish to share with the manufacturers. However, the manufacturers may be willing to make their proprietary data available to be analyzed by the proprietary software of the suppliers and third party experts without exposing the raw data itself to the suppliers and third party experts. In other cases, third party experts and suppliers are willing to allow their proprietary data and software to be used for the analysis of manufacturers' data without exposing the raw proprietary data or logic to the manufacturers. All parties may agree to share data and results of the software operating on the data in a certain manner.

Problems associated with a collaborative working environment involving sharing proprietary data and software between manufacturers third party experts and suppliers include incompatibilities between different data formats and complicated management protocols and access control mechanisms. Further, concerns over the security of the shared data and software, especially transmission of raw real-time data out of the manufacturers' facilities,

BNSDOCID: <WO_____0133759A1_I_>

makes manufacturers reluctant to share detailed, real-time data electronically. Therefore, there is a need for an industry-wide network that allows collection of proprietary information in compatible formats and secure, real-time, event-driven distribution of the proprietary information to network subscribers.

Summary of the Invention

In general, in one aspect, the invention provides a method of sharing data that includes first agreeing upon rules of sharing and then providing a secure escrow zone for collecting and distributing data. The escrow zone includes a first database and an access control program for implementing the agreed upon rules. Next a first set of data from a first network is selected by passing them through a first data filter. The first set of filtered data is then transmitted from the first network to the escrow zone via a secure transmission mode and are deposited in the first database. The first set of filtered data are then accessed by accessing the first database and the access is controlled by the access control program according to the agreed upon rules.

Implementations of this aspect of the invention may include one or more of the following features. The escrow zone may also include a second data filter for protecting the data flow in and out of the escrow zone. The first and second data filters may include a messaging middleware software. The first and second data filters may also include a table of rules defining policies regarding permissibility of data, information and applications programs attempting to cross the filters. The first and second data filters may further have a program to check message headers including identifications for each company, machine, production facility, machine supplier company, message type, message source and message purpose. The data may include proprietary information. The data may be real-time data. The sharing of data occurs between users subscribing to the escrow zone and accepting the agreed upon rules. The subscribing users may be selected from a group including manufacturers, suppliers, vendors, sales representatives, consultants, technical experts and financial analysts. The first set of filtered data may include at least one of machine status, process parameters, quality control data, product specifications, equipment specification, workflow data and company specific financial information. Accessing of data may include retrieving data from the first database and altering of data. The method may also include after depositing the data in the first database recording the deposition time, date, size, content, subject matter and user identification. The secure transmission mode includes first encrypting the first set of filtered

BNSDOCID: <WO_____0133759A1_I_>

data and then transmitting them via an internet network. The escrow zone may be located at the first network or at a third network different from the first. The data may be accessed remotely via an internet network, telephone line and a wireless connection. The method may further include selecting a second set of data from a second network by passing them through a second data filter, transmitting them to the escrow zone via a secure transmission mode and depositing them in the first database. First and second users connected to the first and second networks, respectively, may access the first database and the first and second set of filtered data. The first network may be located at a manufacturing company. The second network may be located at an equipment supplying company. The escrow zone may be located at the second network. The escrow zone may further include a people profile managing software and a people profile database.

In general, in another aspect, the invention features a method of sharing data that includes first agreeing upon rules of sharing and then providing a secure escrow zone for collecting and distributing data. The escrow zone includes a first database and an access control program for implementing the agreed upon rules. Next a plurality of data from a plurality of networks are selected by passing them through a plurality of filters. The plurality of filtered data are then transmitted from the plurality of local networks to the escrow zone via a secure transmission mode and are deposited in the first database. The plurality of filtered data are then accessed by accessing the first database and the access is controlled by the access control program according to the agreed upon rules. A user connected to at least one of the local networks may access the plurality of data.

In general, in another aspect, the invention features an escrow zone system for maintaining proprietary information and data. The escrow zone system includes a database and an access control program. Proprietary information and data are stored in the database. Access to the database is controlled by the access control program.

Implementations of this aspect of the invention may include one or more of the following features. The escrow zone may also include a data filter for protecting the data flow in and out of the escrow zone. The data filter may include a messaging middleware software, a table of rules defining policies regarding permissibility of data, information and applications programs attempting to cross the filter and a program to check message headers including identifications for each company, machine, production facility, machine supplier company,

BNSDOCID: <WO_____0133759A1_I_>

message type, message source and message purpose. The escrow zone system may further include a people profile managing program, a people profile database, an operating system and a local area network system connecting the database to a server hosting the access control program, the profile managing program and the database.

Among the advantages of this invention may be one or more of the following. The system provides non-invasive business to business communication and collaboration via an internet network. It offers standard or custom views of shared real-time data and reports to subscribing companies. The system also offers analytical tools and other shared software that allow exchange of proprietary data according to prearranged rules.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and description below. Other features, objects and advantages of the invention will be apparent from the following description of the preferred embodiments, the drawings and from the claims.

Brief Description of the Drawings

FIG. 1 is a flow diagram of a method for sharing proprietary intellectual property (IP) data;

FIG. 2 is a schematic overview diagram of an escrow zone for sharing proprietary intellectual property data;

FIG. 3 is a schematic overview diagram of another design of an escrow zone for sharing proprietary intellectual property data;

FIG. 4 is a Venn diagram representing an IP escrow zone;

FIG. 5 is a schematic overview diagram of a network system including a manufacturer's local hub, a supplier's local hub and a central hub;

FIG. 6 is a flow diagram of an access control program for the escrow zones of FIGS. 2 and 3;

FIG. 7 is a schematic diagram of an access control program for the escrow zones of FIGS. 2 and 3;

BNSDOCID: <WO_____0133759A1_I_>

FIG. 8 is a flow diagram for entering a user into the network system of FIG. 5;

FIG. 9 is a flow diagram for validating a user entering the system of FIG. 5 through the central hub;

FIG. 10 is a flow diagram for validating a user entering the system of FIG. 5 through the local hub;

FIG. 11 is a screen display of a webpage of "AvantNet Profile Manager"; and

FIG. 12 is a screen display of a webpage of "AvantNet Profile Manager" depicting user assignment information.

Detailed Description of the Invention

Referring to FIG. 1, a method for sharing proprietary information, data and applications programs between two companies includes first deciding upon intellectual property (IP) ownership, establishing rules of sharing and accessing 10. Next an IP escrow zone is provided for storing proprietary information, data and applications programs 20. Next all proprietary information, data and applications programs are collected from the two companies that have accepted the rules of sharing and are transmitted to the IP escrow zone 30. Next all proprietary information, data and applications programs are deposited in the IP escrow zone and the applications programs are enabled to operate on the data 40. The IP escrow zone is then accessed to retrieve the deposited proprietary information, data and applications programs 50. In the financial industry, "escrow" is an account where a third party holds funds on behalf of two or more parties involved in a transaction. In connection with intellectual property assets an IP escrow zone is a digital storage space where two or more companies deposit data and applications programs and are allowed to access each other's deposited data and applications programs based on a contractual arrangement. The IP escrow zone is maintained by a third party. An access control program controls the accessing of the escrow zone and the proprietary information and data 60.

The rules of sharing include what information, data and applications programs are shared, who has access to the shared information, when and where is the information available, the

BNSDOCID: <WO_____0133759A1_I_>

format in which information is available, whether the information is available in absolute units of measure or only relative units such as offsets from or percentages of target values, the conditions under which normal or exceptional sharing is allowed and how information is accessed. The IP escrow zone includes at least a database for storing shared information, data and applications programs and an access control program. One or more data sources associated with the one or more companies that have accepted the escrow agreement, respectively, send data to the database. A filter selects which data are allowed to flow into or out of the IP escrow zone. The data transmission occurs over a public internet network via a secure transmission mode. The filtered data are deposited in the database and a record is created summarizing the time and date of deposition, type of data, subject matter and origin of data. An agreed upon set of operations and analysis is performed on the data by the stored applications programs. A user accesses the data and the results of the applications programs by accessing the escrow zone and the access is controlled by the access control program.

Referring to FIG. 2, a local hub network 110 includes proprietary applications and database modules 220 and 220A and a shared applications and database module 210. Each module 210, 220A and 220 includes a computer server 41, 42, 43 and a database 41A, 42A, 43A, respectively. Local hub 110 is located at a manufacturing facility and collects data from a sensor 44 and a factory local area network (LAN) 240. Sensor 44 is located in machine 212 and transmits data to the local hub 110 via a sensor data link 125. Data from the factory LAN are transmitted to the local hub 110 via a factory data link 135. Modules 210, 220A and 220 are connected to a local hub LAN 251. Local hub LAN 251 also connects to an internet network 160. Local hub 110 is separated from an internet network 160 by a firewall 162. Data flow from the internet network 160, sensor data link 125 and factory data link 135 into the local hub 110 pass through an external data filter 270, a sensor data filter 240 and a factory data filter 250, respectively. In one example, the sensor 44 is an optical sensor located in a chemical vapor deposition (CVD) chamber 212 used in the manufacturing facility where the local hub 110 is located, the internet network 160 is the global TCP-IP Internet and the local area network is an Ethernet LAN. Firewall 162 is a computer that serves to insulate and protect the local hub 110 and its data. It provides security and/or encryption of the data transmitted to or received by the local hub 110 from the internet network 160. An example of such a device is the SonicWALL Pro, supplied by SonicWALL, Inc.

3NSDOCID: <WO_____0133759A1_I_>

Computer servers 41, 42, 43 are computers running an operating system and host applications programs. In one example, the operating system is Microsoft™ Windows NT™. Server 41 hosts applications programs that are shared by all parties having access to the local hub 110. The shared applications programs include database management, data collection and routing and notification. Database 41A is attached to server 41 and stores data that are shared by all parties having access to the local hub 110. Servers 42 and 43 host applications programs specific to running the operations and equipment in the manufacturing facility. In one example, the specific application is a software used by the supplier of the CVD chamber 212 to achieve run-to-run consistency by compensating for minor input variations. In another example, the specific application program is an equipment monitor program that an equipment maintenance service provider uses to monitor the machine's internal vital signs and to detect performance degradation or outright failures. Database 42A is attached to server 42 and stores data associated with the applications programs that are hosted in server 42. In one example, these data are proprietary machine performance data that the supplier of the machine collects and does not wish to share with the manufacturer that uses the machine or other third parties. Database 43 is attached to server 43 and stores data associated with the applications programs that are hosted in server 43. In one example, these data are proprietary data on machine consumables usage that the supplier of the consumables collects and does not wish to share with the manufacturer that uses the machine or other third parties.

Sensor data filter 240, factory data filter 250 and external filter 270 have hardware and software components that mediate the flow of data between the local hub 110 and machine 212, factory LAN 240 and a third party accessing the local hub via the internet network 160, respectively. The hardware components include a server and associated equipment, running an operating system such as Linux and a firewall server running a software program such as Firewall-1 provided by CheckPoint of Redwood City, CA. The software component is a messaging middleware application that is used in the communications between data sources attached to factory LAN 240 and local hub LAN 251. In one example, the messaging middleware application is The Information Bus (TIB) supplied by TIBCO Software, Inc., of Palo Alto, CA. Each communication between data sources or publishers on one side of a filter and data consumers or subscribers on the other side of a filter has an attached header. The attached header follows a naming scheme that is understood by the filter. In one example, the header includes the manufacturing company identification (ID), the manufacturing facility ID, a machine ID, machine supplier company

BNSDOCID: <WO_____0133759A1_I_>

ID, a message type ID, a message source ID and a message purpose ID. Each filter has an associated rules table that defines the policy regarding the permissibility of each message attempting to cross the filter. In one example, the factory data filter 250 prohibits passage of data from the factory LAN 240 to the local hub LAN 251, if the message source is the factory scheduling system and the message type is not machine maintenance request and the message purpose is not to schedule a preventive maintenance procedure with the machine supplier' scheduling system. In another example, the external data filter 270 prohibits passage of a message if the message source is a sensor attached to a specific machine and the data type is raw sensor data. The software components of the filter include software programs that use the message header and naming schemes of the messaging middleware to decide whether or not to allow passage of each message. In one example this is accomplished by using the Entitlements feature of TIB supplied by TIBCO Software, Inc., of Palo Alto, CA. The specific configuration of the applicable rules table is typically determined by contractual arrangement between the production facility and the vendors and suppliers with whom the data will be exchanged.

Referring to FIG. 3, local hubs 110 and 120 are connected to an intellectual property escrow zone 150 via an internet network 160. The intellectual property escrow zone 150 includes a central hub local area network (LAN) 440, a server hosting shared applications and associated databases 420, an access control program 86 and a server hosting proprietary applications and their associated databases 410. Data from local hub 110 pass through a local hub external data filter 270 and a local hub firewall 162 and are transmitted via an internet network 160 to the intellectual property escrow zone 150. Similarly data from local hub 120 pass through a local hub data filter 270A and a local hub firewall 162A and are transmitted via an internet network 160 to the intellectual property escrow zone 150. Data flow from and to the intellectual property escrow zone 150 is also protected by a firewall 166 and a data filter 78. In one example, firewalls 162, 162A, 166 are the security and encryption programs Firewall-1 provided by CheckPoint of Redwood City, CA, the access control program is SiteMinder, supplied by Netegrity, of Waltham, MA and the software filters 270, 270A, 78 are TIB, supplied by TIBCO Software Inc., of Palo Alto, CA..

Figure 4 is a Venn diagram that shows how data, applications and the IP property that is contained in data and applications are shared among three parties in an IP escrow arrangement. The three parties include a factory 200, a vendor 435 and a supplier 300. The

BNSDOCID: <WO_____0133759A1_I_>

three parties share data and applications hosted in the IP escrow zone 150. A machine 212 located in factory 200 also sends data directly to IP escrow zone 150. IP escrow zone 150 represents the logical space managed by the hardware and software of the present invention, including shared applications and data residing on local hubs associated with the factory 200, vendor 435 and supplier 300. Machine 212 represents data transmitted from or to a production machine. Data received from a machine include operating parameters, settings and sensor outputs. Data transmitted to a machine include queries and control commands. Factory 200 represents the logical space occupied by a production facility. Supplier 300 represents the logical space of a supplier. Vendor 435 represents the logical space of a vendor.

The IP escrow zone 150 further includes machine data 200A, supplier applications and data 300A, and vendor applications and data 435A. Machine data 200A represents the intellectual property residing in or derived from applications or data within machine 212. Supplier applications and data 300A represents the intellectual property residing in or derived from the supplier's applications and data. Vendor applications and data 435A represents the intellectual property residing in or derived from the vendor's applications and data. The ellipses representing machine data 200A, supplier applications and data 420, and vendor applications and data 430 are further divided into regions A 450, B 455, C 460, D 465, E 470, F 480, and G 490. Region A 450, which is machine data 200A less regions B 455 and D 465, represents the proprietary intellectual property space of the production facility 200, which is available only to the factory 200. The information within this region is not shared with outside parties. Region B 455, which is the intersection of machine data 200A and supplier applications and data 300A, represents the intellectual property space shared between the factory 200 and the supplier 300 under the escrow arrangement. Region C 460 represents the intellectual property space that the supplier 300 chooses to keep proprietary, and which is not shared with any other parties to the escrow agreement. It is accessed only by the supplier 300. Region D 465 is similar to region B 455. It represents the intellectual property space shared between the factory 200 and the vendor 435 under the escrow arrangement. These data are available only to the factory 200 and the vendor 435. Region E 470 represents the intellectual property space that the vendor 435 chooses to keep proprietary and is not shared with any other parties to the escrow agreement. It is accessed only by the vendor 435. Region F 480 represents the intellectual property space shared among all three parties of the escrow arrangement. These data are provided to and shared between the factory 200, the

BNSDOCID: <WO_____0133759A1_I_>

supplier 300 and the vendor 435. Region G 490 represents the intellectual property space shared between the supplier 300 and the vendor 435 under the escrow arrangement. This space is only accessible by the supplier 300 and the vendor 435, although the factory 200 may provide inputs to the applications running in this space.

Referring to FIG. 5, local hub 110 is installed at a manufacturer's site and serves the purpose of centralizing all the local data, information and communication protocols. In one example, local hub 110 supports data and information associated with a semiconductor fabrication operation 200. The semiconductor fabrication operation 200 includes a manufacturing line 210 that produces integrated circuit devices ("chips"), a resource planning system 222 that plans and coordinates the production operation, a database 221 for storing all the data associated with the semiconductor fabrication operation 200 and a local area network (LAN) 240 that provides connectivity between the manufacturing line 210, the resource planning system 222 and the database 221. In one example, the local area network 240 is an Ethernet LAN and the resource planning system 222 is an Enterprise Resource Planning(ERP) system. The manufacturing line 210 includes a chemical vapor deposition (CVD) chamber 212 for depositing thin films on semiconductor wafers, a photolithography station 214, a chemical mechanical polishing (CMP) apparatus 216 and a quality control and packaging station 218. Control units 213, 215, 217 and 219 for the CVD chamber 212, the photolithography station 214, the CMP apparatus 216 and the quality control and packaging line 218, respectively, are connected to the LAN network 240 via a data link line 232. Examples of control units 213, 215, 217 and 219 include programmable logic controllers (PLC), microcomputers, and computer workstations. Examples of a data link 232 include optical interfaces and electrical interfaces.

LAN network 240 connects to the local hub 110 through a local hub network 251. Similarly, the resource planning system 222 and the database 221 are connected to the local hub network 251 through the LAN network 240. Local hub 110 serves as the local control and data acquisition station for the semiconductor fabrication operation 200. Operators, manufacturing managers, engineers, sales and business managers associated with the semiconductor fabrication operation 200 have access to the production operation through their personal computers 245 that are also connected to the local hub 110 via the local hub network 251. In other embodiments personal computers 245 are connected to the LAN network 240. The semiconductor quality control and packaging station 218 connects also

BNSDOCID: <WO_____0133759A1_I_>

directly to the local hub network 251 via a sensor data link 223. Sensor data link 223 receives data from a sensor (not shown) that is embedded in the packaging station 218 and transmits them to the local hub 110. Sensors embedded in the packaging station 218 include optical, electrical and magnetic sensors.

Local hub 120 is installed at a supplier's site and serves the purpose of centralizing all the local data, information and communication protocols. In one example, local hub 120 is located at an equipment supplier company 300 that supplies the above-mentioned CVD chamber 212. The operation at equipment supplier 300 includes R&D and customer support system 309 for the CVD chambers, a failure diagnostic system 319 that facilitates trouble shooting the CVD chamber operation, a database 330 for storing all the data associated with the CVD chamber operation and diagnosis and a local network 305 that provides connectivity between the CVD customer support system 309, the failure diagnosis system 319 and the database 330. The CVD chamber customer support system 309 is connected to the local hub 120 via the local hub network 340 and the local net 305. The failure diagnostic system 319 and the database 330 are also connected to the local hub 120 through the local hub network 340 and the local net 305. Local hub 120 serves as the central local control station for the CVD chamber supplier 300. Customer support staff, engineers, sales and business managers associated with the CVD chamber supplier company 300 have access to the customer support system 309 through personal computers 345 that are also connected to the local hub network 120 via the local hub network 340 and the local net 305. Local hub 120 has also it's own security system that provides security, authorization and access control for customer support staff, engineers, sales and business managers associated with the CVD chamber supplier company 300.

Local hub 110 of the semiconductor fabrication operation 200 and local hub 120 of the CVD chamber supplier are connected to a central hub 150 via an internet network 160. Security firewalls 162, 164 and 166 are installed between the local hub 110 and the internet network 160, between the local hub 120 and the internet network 160 and between the central hub 150 and the internet network 160, respectively. In one example, internet network 160 is the "Internet" and firewalls 162, 164 and 166 are computers or other digital appliances that run security and encryption software programs. The purpose of the firewalls 162, 164 and 166 is to control and prevent access to the local hubs 110, 120, and central hub 150 by unauthorized external users. Data transmitted through the firewalls 162, 164 and 166 are

BNSDOCID: <WO_____0133759A1_I_>

encrypted for security purposes. In one example, the firewall security and encryption program is Firewall-1 provided by CheckPoint of Redwood City, CA.

Central hub 150 is located at the network provider's site, i.e., AvantNet, and includes a central database 430, a messaging server 410, an application server 420, a data replication server 415 and a LAN network 440 connecting the central database 430 and servers 410, 415 and 420. A firewall 166 is installed between the central hub 150 and the internet network 160. Application server 420 includes a computer server and associated equipment, running an operating system and applications that can be accessed and shared between the local hubs 110 and 120 and other authorized and authenticated users 125 accessing the central hub via the internet network 160. In one example, the operating system is a Microsoft™ Windows™ NT™ system. Applications running on the application server 420 include access control software, data acquisition software, analytical software, process control software, equipment diagnostic software, process diagnostic software, yield diagnostic software, knowledge databases, routing and notification instructions, equipment repair and maintenance management software, instructions and manuals, supply chain planning, coordination and procurement software, call center applications and problem management applications. Applications running on application server 420 run also on the local hub applications servers 220 and 320. In this way, two layers of application providers are possible, that is an application is hosted at the local hub and the central hub servers. Applications stored at the local hub servers offer a privacy advantage to the manufacturer that houses the local hub, whereas applications stored at the central hub have the advantage of allowing sharing by multiple users. In other embodiments, the above mentioned applications are stored only at the central hub applications server 420 and are accessed and shared by the subscribing local hubs 110, 120.

The central database 430 hosts data from the local hubs 110 and 120 that can be accessed by both the semiconductor fabrication operation 200 and the equipment supplier company 300 based on a contractual arrangement. In some cases a third party 125 is also allowed to access the data stored in the central database 430 based again on contractual arrangements between the third party, the semiconductor fabrication operation 200 and the equipment supplier company 300. The database 430 is managed by database software, such as Microsoft™ SQL Server™. Third party data are also stored at the central database and can be accessed by both the semiconductor fabrication operation 200 and the equipment supplier company 300

BNSDOCID: <WO_____0133759A1_I_>

based on a contractual arrangement. Real time equipment status data flows from the manufacturer site 200 to the supplier site 300 via the central hub 150, shown schematically by arrow 90. Equipment process and maintenance tips, manuals and training material flow from the supplier site 300 to the manufacturer site 200 via the central hub 150, shown schematically by arrow 92.

Data travels along paths 170 and 172 from the local hub 110 to the central hub 150 and back, respectively, and along paths 174 and 176 from the local hub 120 to the central hub 150 and back, respectively. The data flow includes passive listening and retrieving of data and active altering of data and issuing of commands. Both the passive and active flow of data is managed by a messaging middleware application, that is installed in the messaging server 410. In one example, the messaging middleware application is The Information Bus (TIB) supplied by TIBCO Software, Inc., of Palo Alto, CA In some embodiments, the data transfer process is automated. In one example, the data is a user's manual for a piece of equipment, which is stored in the central database 430 and can be accessed by all manufacturer's that use the specific equipment in their operations and have either a local hub connected to the central hub or have remote dial in access to the central hub. Upgrades of the manual are automatically fed to the central database 430 from the equipment supplier 300 and can be accessed by all manufacturers 200 without delay.

A data replication software manages replication and synchronization of data between the local hubs 110, 120 and the central hub 150. The data replication software is installed in the data replication servers 415, 215 and 315 of the central hub server 150 and the local hubs 110 and 120, respectively. Connectivity and administration of the overall network and hub operations are provided by an internet service provider. In one example the internet service provider is EXODUS, Inc located in Santa Clara, California.

Referring to FIGS. 6 and 5, access control is part of an overall security method that also includes authentication and adjudication. A "user" associated with the semiconductor fabrication operation 200 of FIG. 5, i.e., operators, manufacturing managers, engineers, sales and business managers, is assigned a profile that includes a user identification name (ID) and a password. Every time a "user" logs into the local hub 110 through a personal computer 245, he needs to provide his assigned user identification name and password 510. The access control program identifies all the appropriate user profiles, classes of equipment data and

BNSDOCID: <WO_____0133759A1_I_>

application functions that the "user" has access to and allows the "user" to proceed 512. If the user does not belong to any of the identified profiles, access is denied 514. After this authentication process the "user" accesses a subset of application functions that may include listening, retrieving, altering data or issuing a command and class of data 516. Next the "user" selects a specific application function applied to a specific set of data 518. The requested operation is allowed to be executed based on the authentication information combined with the appropriate retrieved access function that was assigned to the specific member that is requesting the operation 520. The access control program then adjudicates the selected operation and based on stored information displays the requested data and application function 522 or denies it 524.

Machine and people profiles are created by local and/or central profile managing software. Local profile manager creates and updates data stored in the local people profile databases 605a, 605b, shown in FIG. 3. Local people profile databases 605a, 605b hold information about who is authorized to use which functionality within which application to view or manipulate which data about which equipment, who has local access and to what, who needs to be alerted internally or externally in case of a problem and who needs to be notified at which escalation level. Central profile manager creates and updates data stored in the central people profile database 627, also shown in FIG. 3. Central people profile database 627 holds information about individual person set-up, individual to company relation, individual to equipment relation, who has central access and to what, company specific alerting and escalation profiles and individual to profile assignment. The central profile manager and the central profile database 627 have similar functionality and data as the local profile manager and local profile database 605. The central profile manager has the additional function of coordinating with the local profile manager in order to disseminate, replicate and synchronize profile changes made to any local database 605a, 605b at any local hub. In one example, changes in access rights and profiles caused by employee turnover at equipment supplier local hub 120 are made available to manufacturer local hub 110 in real time, shown in FIG 5. This is particularly useful if the concerned employee had access rights to local hub 110 because of his or her employment with supplier 300.

Referring to FIGS. 7 and 5, an access control system 86 includes proprietary data 81, agreed upon rules 83, user interfaces 85, people profile database 90, equipment specification database 95 and application functions 96. The applications functions 96 include listening,

BNSDOCID: <WO_____0133759A1_I_>

retrieving, modifying of data and issuing and executing control commands. Accordingly, several access levels are defined by segmenting and grouping the various access application functions 96. User groups, such as operators, manufacturing managers, engineers, sales and business managers associated with the production operation 200, are each assigned one or more appropriate access level group profiles 91. Each individual user 92 is then assigned to one or more group profiles 91. This assignment of access functions to each group profile 91 and the assignment of individual users 92 to group profiles are stored in a people profile database 90. Each profile may be connected to one or more individual users. In addition to a people profile database 90 and the access application functions 96, an access control system 86 includes an equipment specification database 95. Equipment specification database 95 includes the individual machines 94 and also groups or classes of machines 93. The machine classes 93 include individual machines 94. Machines belonging to the same class are subject to the same access control rules. Each individual machine may be assigned to one or more classes. Each class includes one or more machines. All access to data is only permitted via an application. Within each application access to data is further controlled by controlling access to functions of the application. In one example, an application has one function for viewing the machine status and another function for viewing and updating the machine status. Accordingly, an operator having a restricted access profile is only allowed to view a machine status, whereas an operations manager with a more extended access profile is allowed to view and update the machine status. The proprietary information and data 81, the agreed upon rules 83 and the user interfaces 85 are stored in the IP escrow zone at local hub 110 or in the IP escrow zone at the central hub 150 of FIG. 5.

Referring to FIG. 8, the process of entering a new user into a profile database includes the following steps. A local system administrator enters the new user's data at the local hub 101. The new user's data are checked against all stored user's data in the central hub for duplicate entries. A list of close matches is retrieved 112 and one is selected 113. If there is a match all the detailed personal information is downloaded from the central hub 116. If there is no close match 114 central hub issues a new ID 115 and the local system administrator enters new user's data 131. The local system administrator connects the user to a profile 141 and deposits new user's ID and assigned profile in the appropriate company specific database stored in the central hub 118. The new user's ID and assigned profile are also sent to the local profile manager 230. Central profile manager performs periodic profile matching and

BNSDOCID: <WO_____0133759A1_I_>

replication 117 between central hub profiles stored in central database 430 and local hub profiles stored in local hub database 230.

Referring to FIG. 9, when a user logs in 101 the central hub a validation process 111 follows that includes the following steps. First the system checks if there is a user ID matching the user's identification and password in the central hub profile database 121. If the user's ID exists the system identifies a superset or a group of profiles to which the user belongs 131. Next the system identifies a superset of all the applications rights, i.e., all the applications to which the identified group of profiles has access 141. The available applications are then displayed to the user 151. The displays are usually webpages projected in a computer screen, shown in FIGS. 11and 12. The user then selects an application 161. The system determines a superset of function rights, i.e., all the specific functions that the user is allowed to access within a given application for a given class of machine data 171. The highest access for each class is then determined 181. The system then displays a map of the available functions for each class of machine data 191. System runs the selected application 202. If the user's profile does not exist in the system. the user is rejected 201. In this case the user has the option to repeat the login procedure 203 for a preset number of attempts before the user ID is temporarily disabled and an alert is sent to the appropriate security administrator.

Referring to FIG. 10, when a user logs in 101 through a local hub a validation process 111 follows that includes the following steps. First the system checks if there is a profile in the local profile database matching the user's identification and password. If the user's profile exists the system identifies a superset or a group of profiles to which the user belongs 121. Next the system identifies a superset of all the applications rights, i.e., all the applications to which the identified profile has access 131 and displays all available applications to the user 141. The user then selects an application 151. The system determines a superset of function rights, i.e., all the specific functions that the user is allowed to access within a given application for a given class of machine data 161. The highest access for each class of machine data is then determined 171 and the system then displays a map of the available functions for each class of machine data for the selected application 172. The system runs the application 173 .

If the user is a member of the local hub but logs in through the central hub 181, the access control of the central hub performs the authentication process 191, i.e., identification and password. If the profile exists in the central profile database, it is matched with the

BNSDOCID: <WO 0133759A1 I >

appropriate company and local hub 201 and the local hub access control is invoked 121. If the user belongs to a different company and logs in through the central hub 221, the access control of the central hub authenticates the user 231. If the profile exists in the central profile database, it is matched with the appropriate company and local hub 201 and the local hub access control is invoked 121. If the user is a third party, logs in through a local hub 241 and this is not the first time that the user logs in, the request is routed to the central access control 311 where authentication takes place. If the profile exists in the central profile database 321, it is matched with the appropriate company and the local hub access control is invoked 121. If the profile does not match an existing profile in the central profile database, the user is rejected 331. If the user is a third party, logs in through a local hub 241 and this is the first time that the user logs in 251, the local host administrator receives a request to add a new user 261. The local host administrator decides and creates a local hub identification and password 271. The local host administrator then checks the primary company affiliation at the central profile database 280. If there is a match with a profile affiliated with a subscribing company in the central profile database 290, the profile is downloaded to the local hub 301.

Referring to FIGS. 11 and 12, in one example user B is a member of ABC International Corporation and has an assigned profile p1. The central profile manager matches the user B to profile p1 and displays all classes of machine data available to profile p1. Profile p1 has two classes of machine data available, c1 and c2. Class c1 includes data for machines om1, om2, om3 and class c2 includes data for machine om3. A map of all profiles p1, p2, p10, classes per profile c1, c2, c4, c5, c6 and machines per class om1, om2, om3, om4, om5, om6 is also displayed, shown in FIG. 12. In this example, the application is listening and retrieving data of machine om1.

Other embodiments are within the scope of this invention. For example, the IP escrow zone may include more than one databases and servers. The data transmission may occur via a secure private network. Data filters 240, 250 and 270 of FIG. 2 may each include a firewall. More than two local hubs may be connected to the central hub of FIG. 3. A user may be authenticated via a digital certificate, digital key or a smart card, among others. The escrow zone may also hold software programs and data calculated by software programs. The escrow zone may be located in one of the local hubs and managed by the local hub administration.

BNSDOCID: <WO_____0133759A1_I_>

The many features and advantages of the present invention are apparent from the detailed specification, and, thus, it is intended by the appended claims to cover all such features and advantages of the described apparatus that follow the true spirit and scope of the invention. Furthermore, since numerous modifications and changes will readily occur to those of skill in the art, it is not desired to limit the invention to the exact construction and operation described herein. Accordingly, other embodiments are within the scope of the following claims.

BNSDOCID: <WO 0133759A1 I >

What is claimed is:

1. A method of sharing data comprising:
agreeing upon rules of sharing;
providing a secure escrow zone for collecting and distributing data comprising a first database and an access control program for implementing said agreed upon rules;
selecting a first set of data from a first network by passing data through a first data filter;
transmitting said first set of filtered data from said first network to said escrow zone via a secure transmission mode;
depositing said first set of filtered data in said first database: and
accessing said first set of filtered data in said first database wherein said access is controlled by said access control program according to said agreed upon rules.

2. The method of claim 1 wherein said escrow zone further comprises a second data filter for protecting data flow in and out of said first database.

3. The method of claim 2 wherein said first and second data filter comprise a messaging middleware software.

4. The method of claim 3 wherein said first and second data filter further comprise a table of rules defining policies regarding permissibility of data, information and applications programs attempting to cross said filters.

5. The method of claim 4 wherein said first and second data filter further comprise a header including identifications for each company, machine, production facility, machine supplier company, message type, message source and message purpose.

6. The method of claim 1 wherein said first set of filtered data comprise proprietary information.

7. The method of claim 1 wherein said first set of filtered data comprise real-time data.

BNSDOCID: <WO_____0133759A1_I_>

8. The method of claim 1 wherein said sharing of data occurs between users subscribing to said escrow zone and accepting said agreed upon rules.

9. The method of claim 8 wherein said subscribing users are selected from a group consisting of manufacturers. suppliers, vendors. sales representatives. consultants. technical experts and financial analysts.

10. The method of claim 1 wherein said first set of filtered data comprise at least one of machine status, process parameters, quality control data. product specifications, equipment specification, work flow data and company specific financial information.

11. The method of claim 1 further comprising retrieving said first set of filtered data from said first database.

12. The method of claim 1 further comprising altering said first set of filtered data.

13. The method of claim 1 further comprising after depositing said data recording said deposition of data in said first database.

14. The method of claim 13 wherein said recording comprises recording at least one of time, date, size, content, subject matter and user identification.

15. The method of claim 1 wherein said secure transmission mode comprises:
encryption of said first set of filtered data; and
transmission of said encrypted data via an internet network.

16. The method of claim 1 wherein said escrow zone is located at said first network.

17. The method of claim 1 wherein said escrow zone is located at a third network.

18. The method of claim 1 wherein said data are accessed remotely via an internet network.

19. The method of claim 1 wherein said data are accessed remotely via a telephone line.

BNSDOCID: <WO 0133759A1 I >

20. The method of claim 1 wherein said data are accessed remotely via a wireless connection.

21. The method of claim 1 further comprising:
selecting a second set of data from a second network by passing them through a third data filter;
transmitting said second set of filtered data from said second network to said escrow zone via a secure transmission mode;
depositing said second set of filtered data in said first database; and
wherein a first and second users connected to said first and second networks, respectively, have access to said first database and said first and second set of filtered data.

22. The method of claim 1 wherein said first network is located at a manufacturing company.

23. The method of claim 21 wherein said second network is located at an equipment supplying company.

24. The method of claim 21, wherein said escrow zone is located at said second network.

25. A method of sharing data comprising:
agreeing upon rules of sharing;
providing a secure escrow zone for collecting and distributing data comprising a first database and an access control program for implementing said agreed upon rules;
selecting a plurality of data from a corresponding plurality of networks by passing them through a corresponding plurality of data filters;
transmitting said plurality of filtered data from said plurality of networks to said escrow zone via a secure transmission mode;
depositing said plurality of filtered data in said first database; and
accessing said plurality of filtered data in said first database wherein said access is controlled by said access control program according to said agreed upon rules.

26. The method of claim 25 wherein said escrow zone is located at a central network connected to said plurality of networks via an internet network.

BNSDOCID: <WO_____0133759A1_I_>

27. The method of claim 25 wherein said escrow zone is located at one of said plurality of networks.

28. The method of claim 25 wherein said data are accessed by a user connected to at least one of said plurality of networks.

29. The method of claim 1 wherein said escrow zone further comprises a people profile managing software.

30. The method of claim 1 wherein said escrow zone further comprises a people profile database.

31. An escrow zone system for maintaining proprietary information and data comprising:
a database;
an access control program; and
wherein said proprietary information and data are stored in said database and access to said database is controlled by said access control program.

32. The escrow zone system of claim 31 further comprising a data filter for protecting data flow in and out of said database.

33. The escrow zone system of claim 32 wherein said data filter comprises a messaging middleware software.

34. The escrow zone system of claim 33 wherein said data filter further comprises a table of rules defining policies regarding permissibility of data, information and applications programs attempting to cross said filters.

35. The escrow zone system of claim 33 wherein said data filter further comprises a software program for checking message headers including identifications for at least one of company, machine, production facility, machine supplier company, message type, message source and message purpose.

BNSDOCID: <WO 0133759A1 I >

36. The escrow zone system of claim 30 further comprising a people profile managing program.

37. The escrow zone system of claim 30 further comprising a people profile database.

38. The escrow zone system of claim 30 further comprising an operating system.

39. The escrow zone system of claim 30 further comprising a local area network connecting said database to a server hosting said access control program.

BNSDOCID: <WO_____0133759A1_I_>

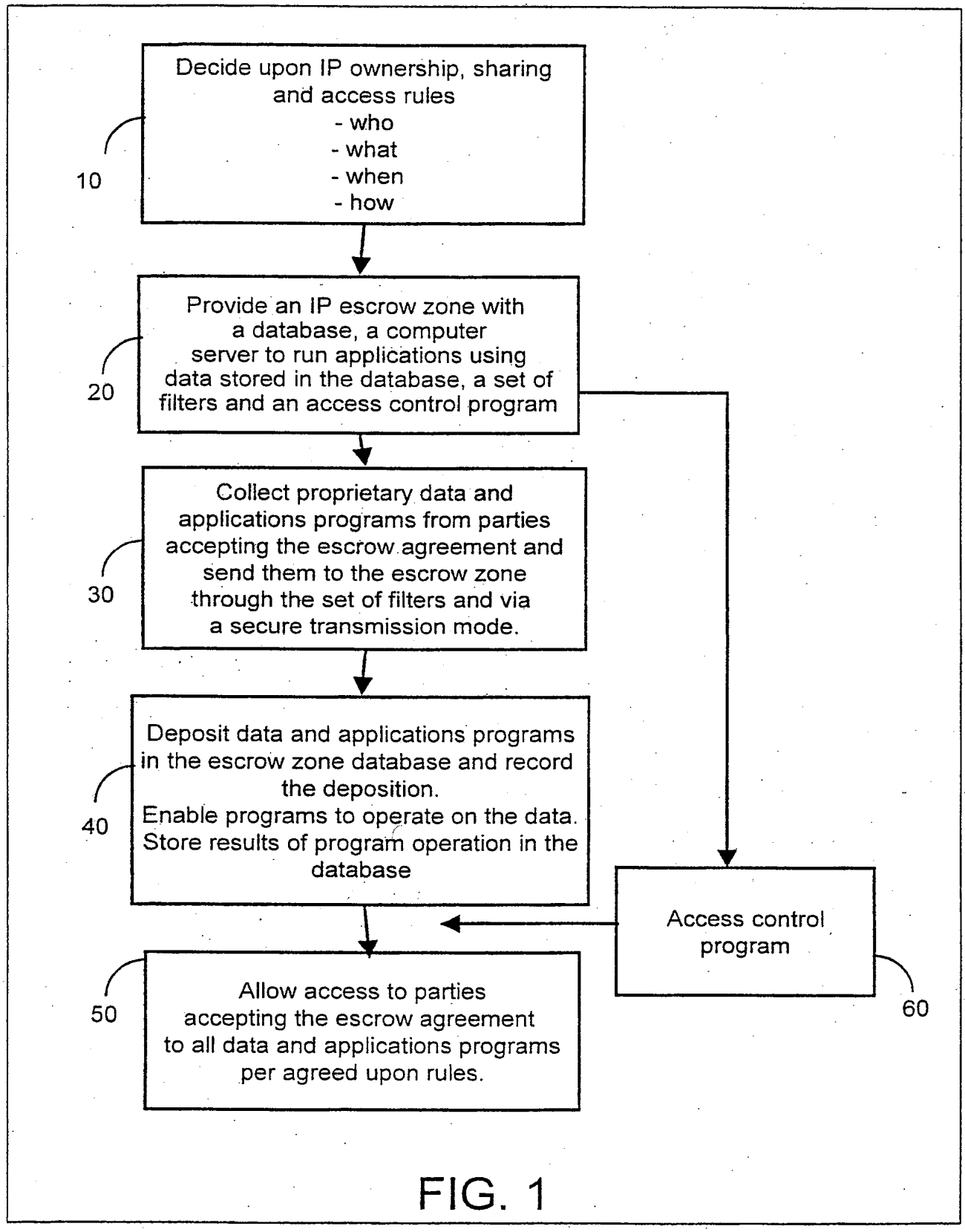


FIG. 1

BNSDOCID: <WO_____0133759A1_I_>

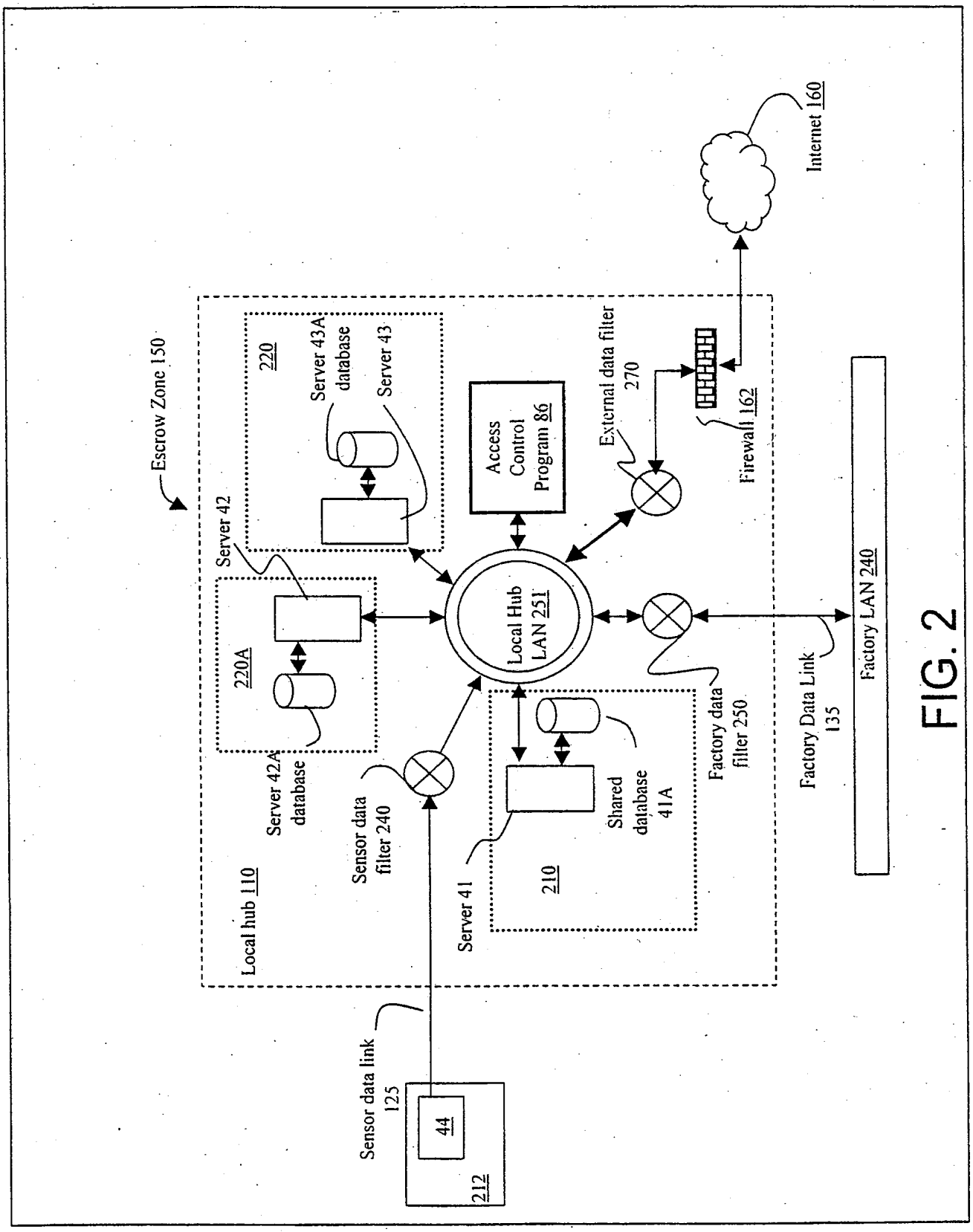


FIG. 2

BNSDOCID: <WO_____0133759A1_I_>

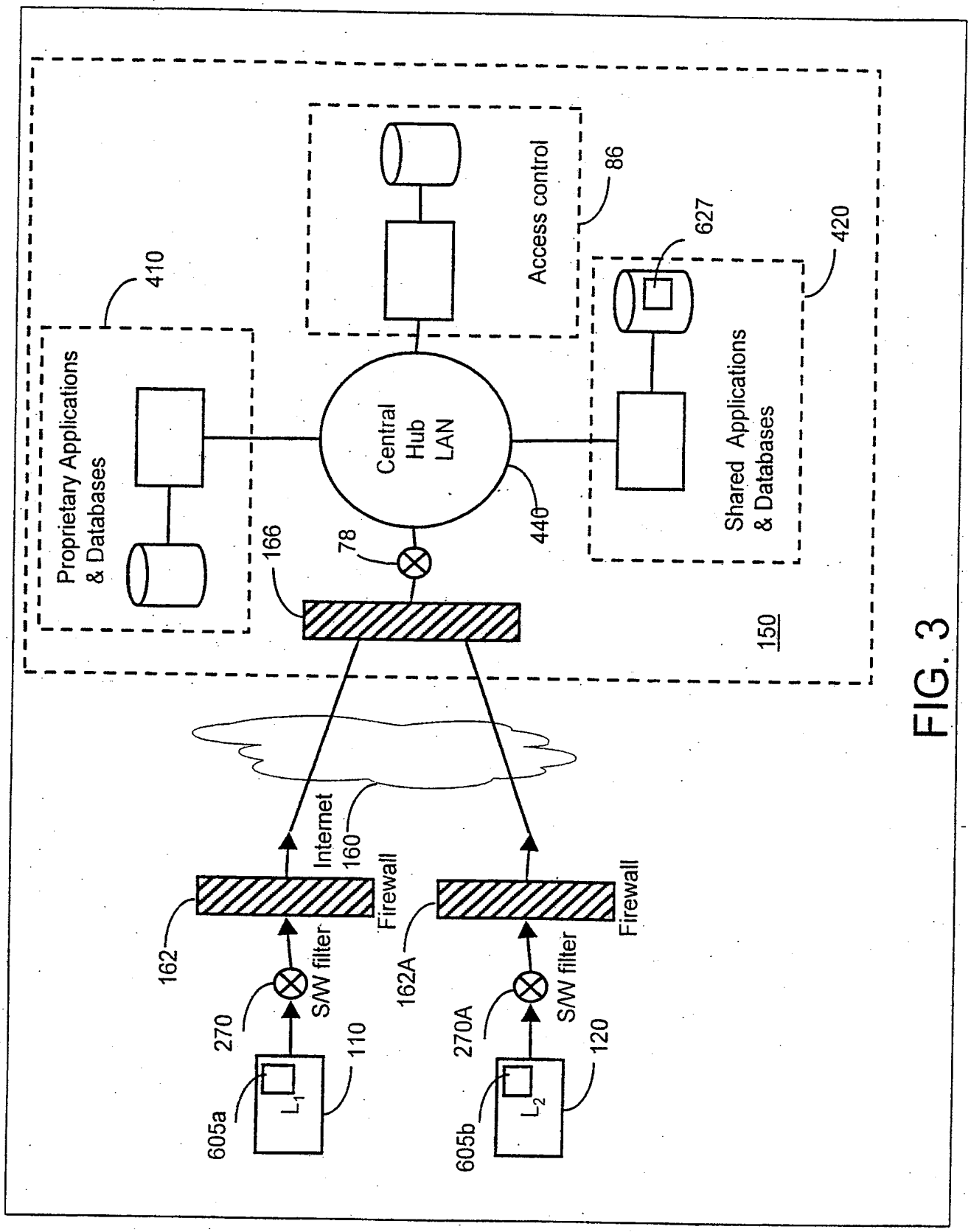

Access control
86
627
420
410
Proprietary Applications & Databases
Central Hub LAN
440
Shared Applications & Databases
78
166
150
Internet
160
Firewall
Firewall
162
162A
S/W filter
S/W filter
270
270A
110
120
605a
605b
L_1
L_2

FIG. 3

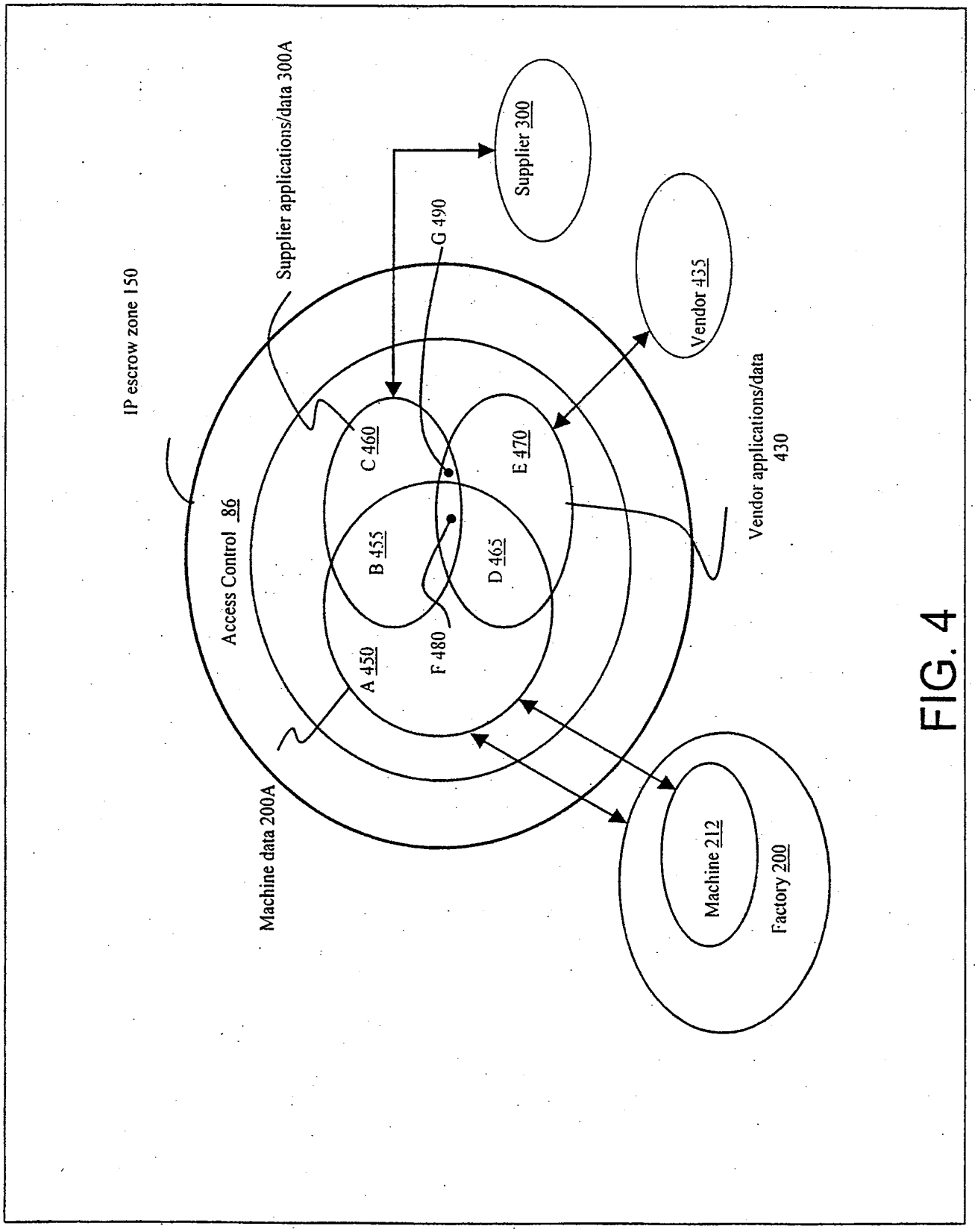
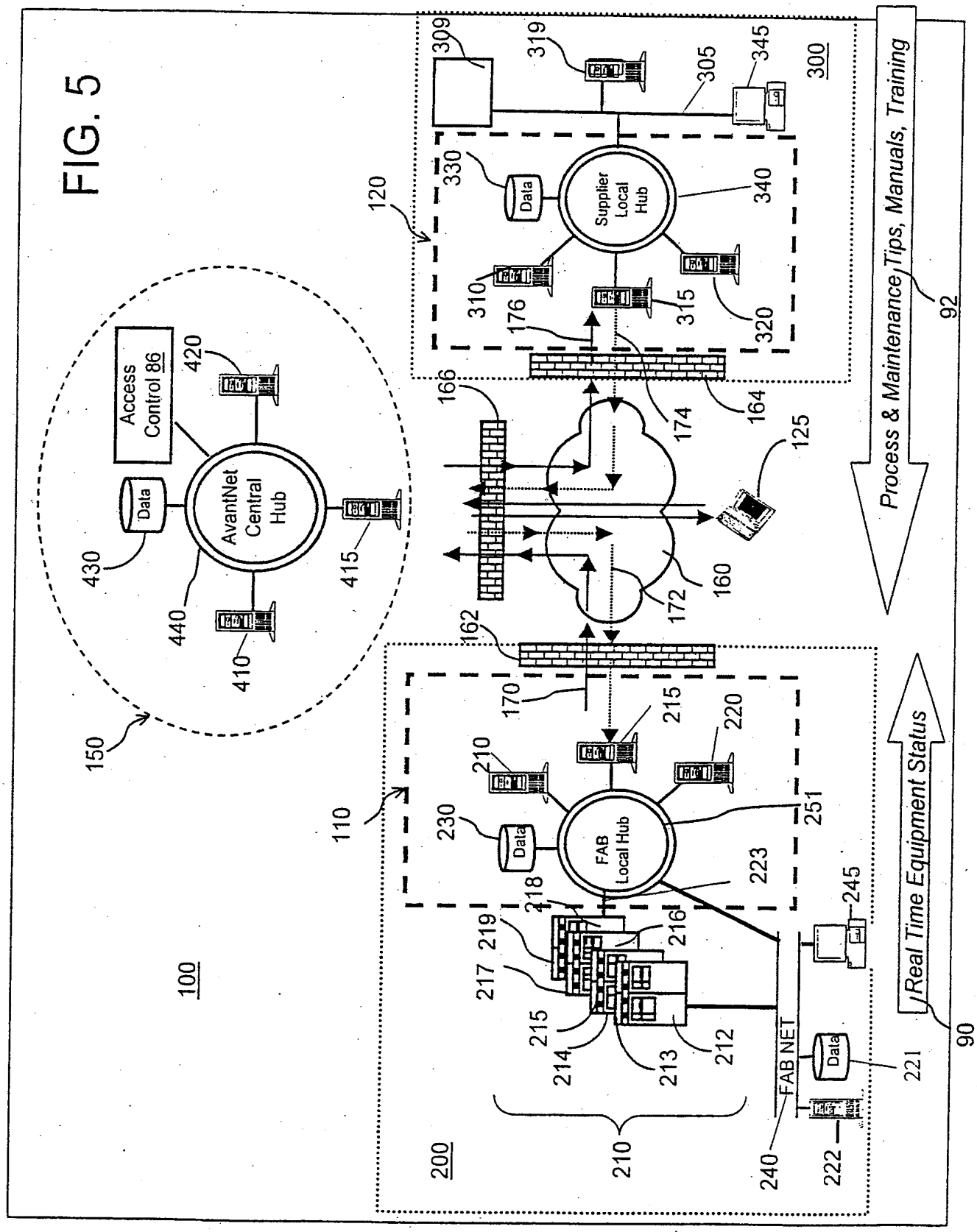


FIG. 4

BNSDOCID: <WO_____0133759A1_I_>

FIG. 5



BNSDOCID: <WO 0133759A1 | >

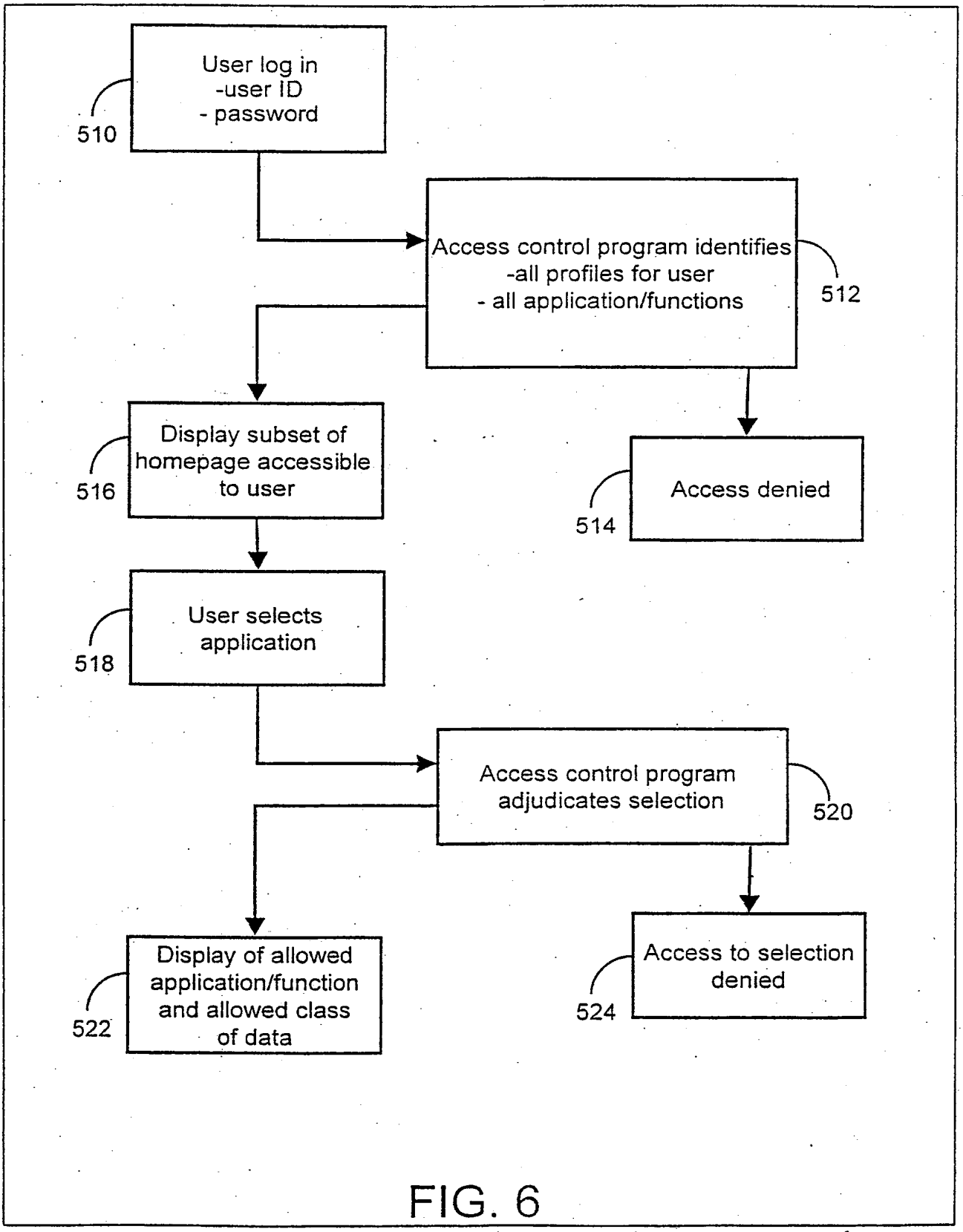


FIG. 6

BNSDOCID: <WO_____0133759A1_I_>

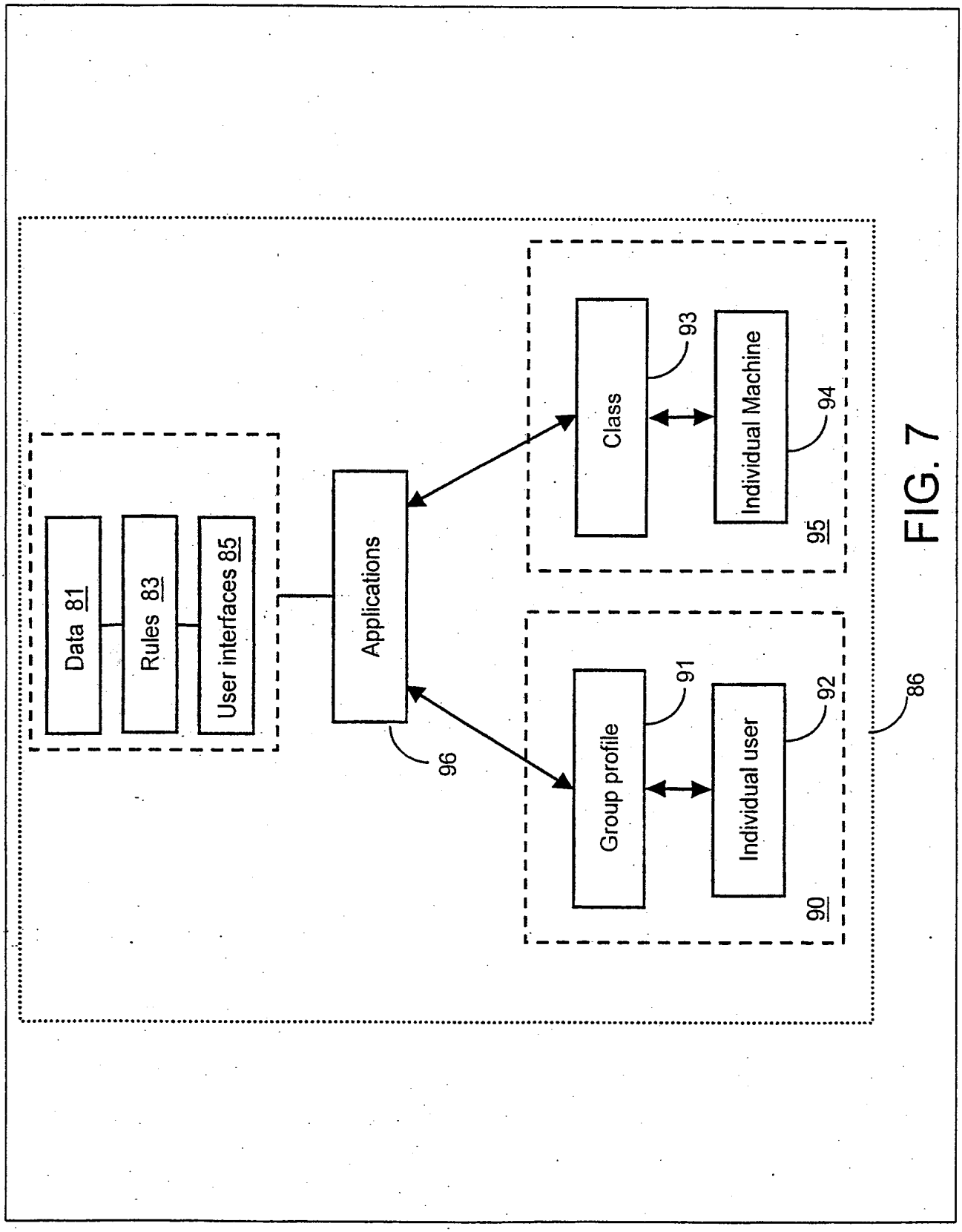

Data 81
Rules 83
User interfaces 85
Applications
96
Class
93
Individual Machine
94
95
Group profile
91
Individual user
92
90
86

FIG. 7

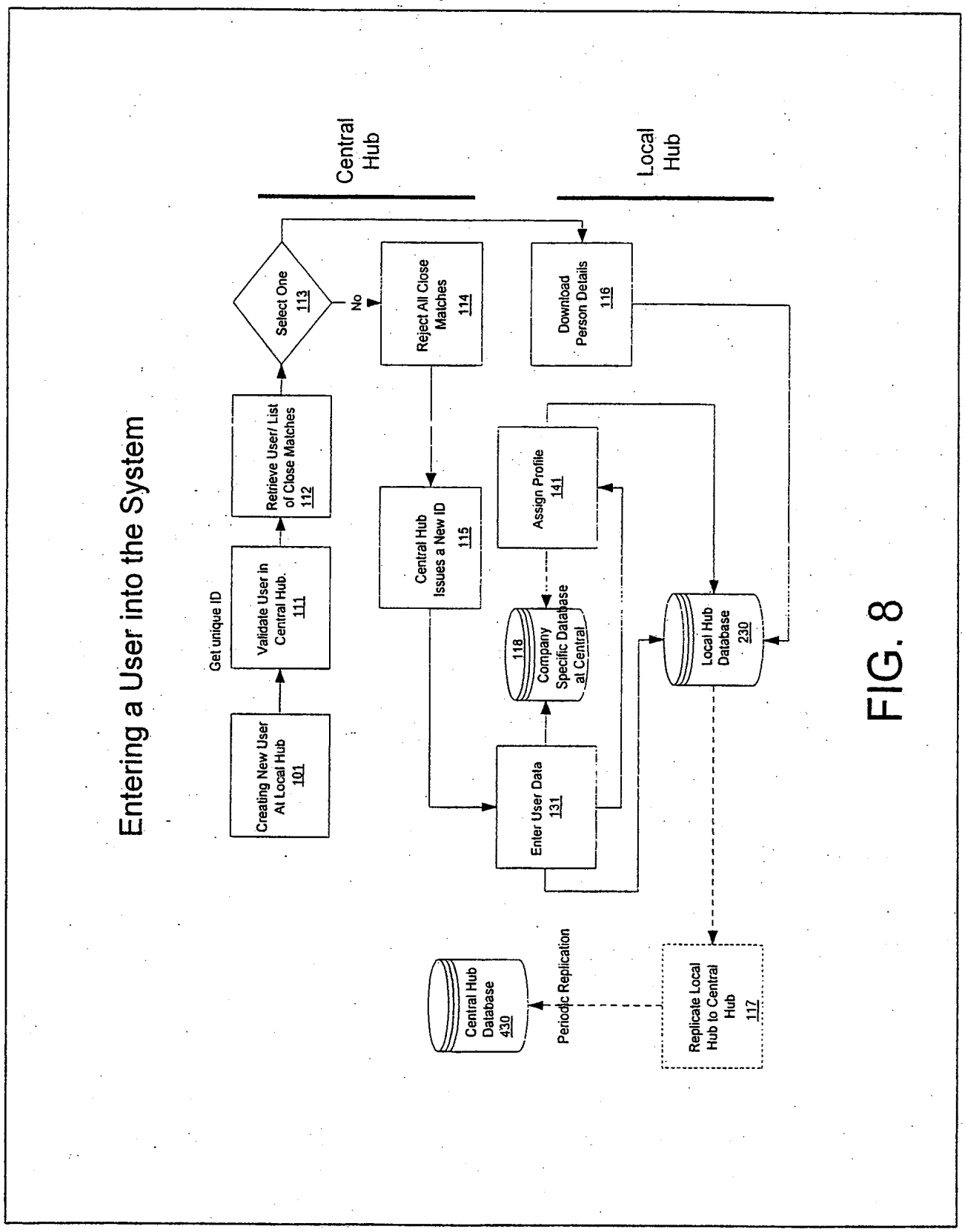


FIG. 8

BNSDOCID: <WO_____0133759A1_I_>

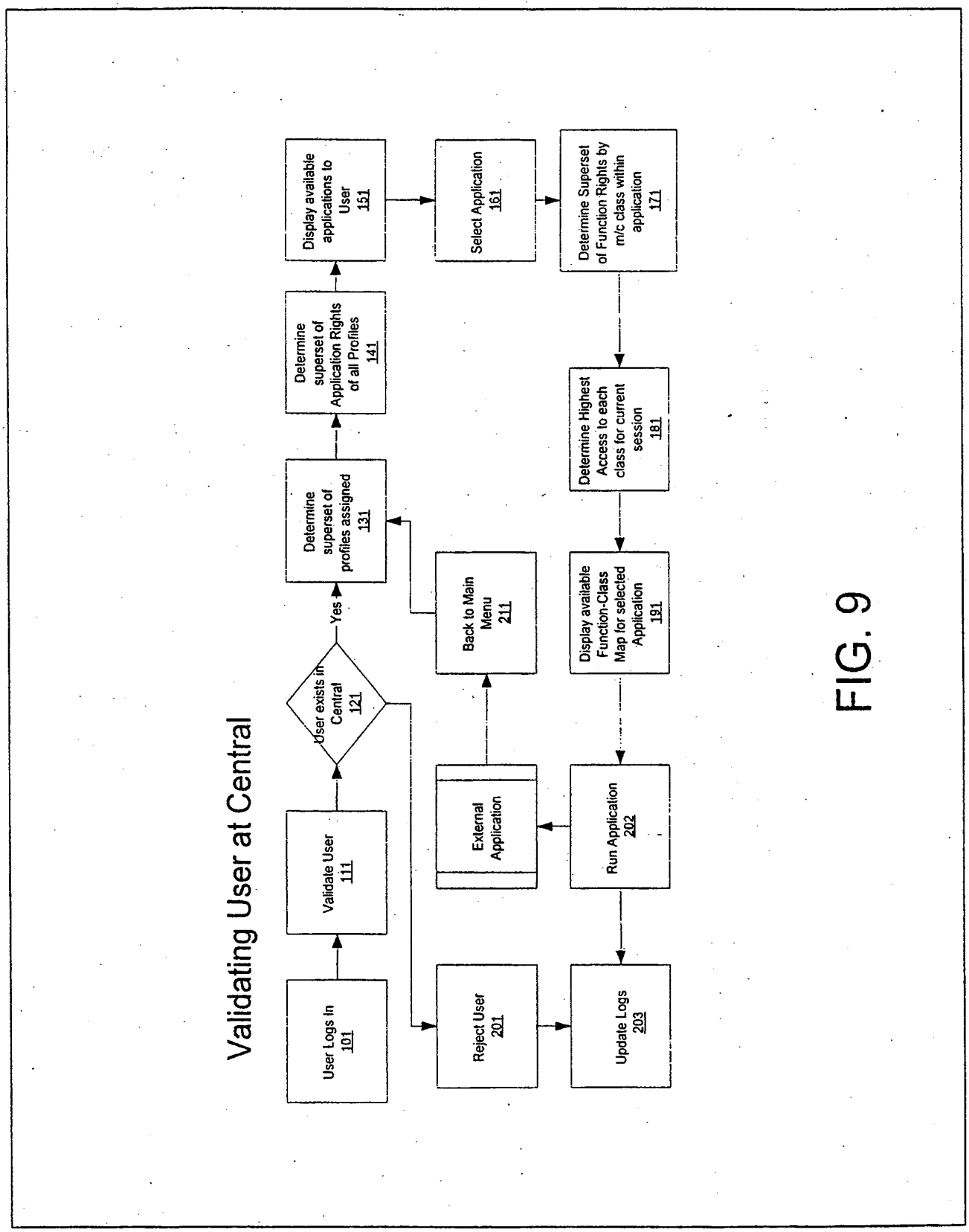


FIG. 9

BNSDOCID: <WO 0133759A1 >

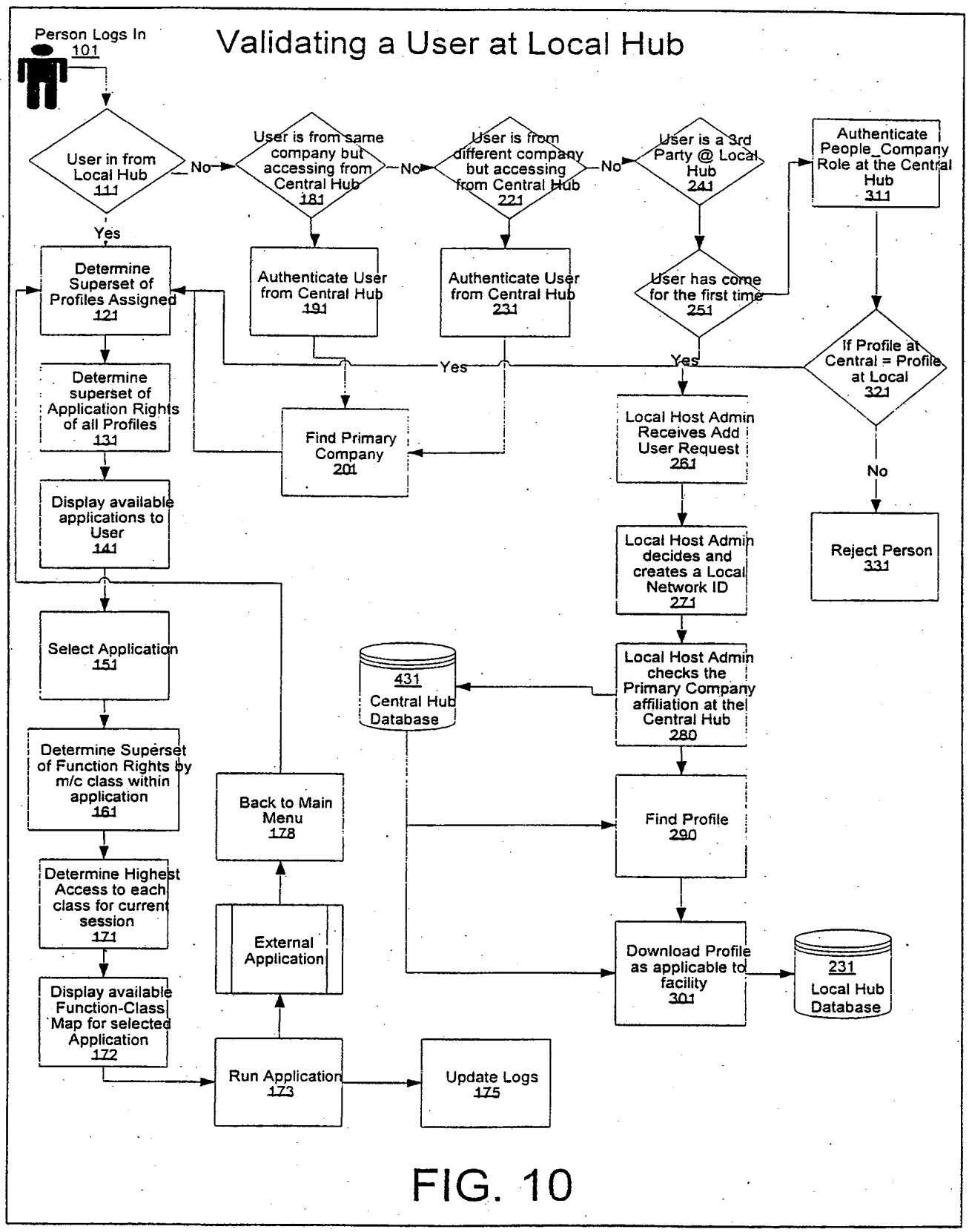

Validating a User at Local Hub
Person Logs In
101
User in from Local Hub
111
No
User is from same company but accessing from Central Hub
181
No
User is from different company but accessing from Central Hub
221
No
User is a 3rd Party @ Local Hub
241
Authenticate People_Company Role at the Central Hub
311
Yes
Determine Superset of Profiles Assigned
121
Authenticate User from Central Hub
191
Authenticate User from Central Hub
231
User has come for the first time
251
Yes
If Profile at Central = Profile at Local
321
Yes
Determine superset of Application Rights of all Profiles
131
Find Primary Company
201
Local Host Admin Receives Add User Request
261
No
Display available applications to User
141
Local Host Admin decides and creates a Local Network ID
271
Reject Person
331
Select Application
151
431
Central Hub Database
Local Host Admin checks the Primary Company affiliation at the Central Hub
280
Determine Superset of Function Rights by m/c class within application
161
Back to Main Menu
178
Find Profile
290
Determine Highest Access to each class for current session
171
External Application
Download Profile as applicable to facility
301
231
Local Hub Database
Display available Function-Class Map for selected Application
172
Run Application
173
Update Logs
175

FIG. 10

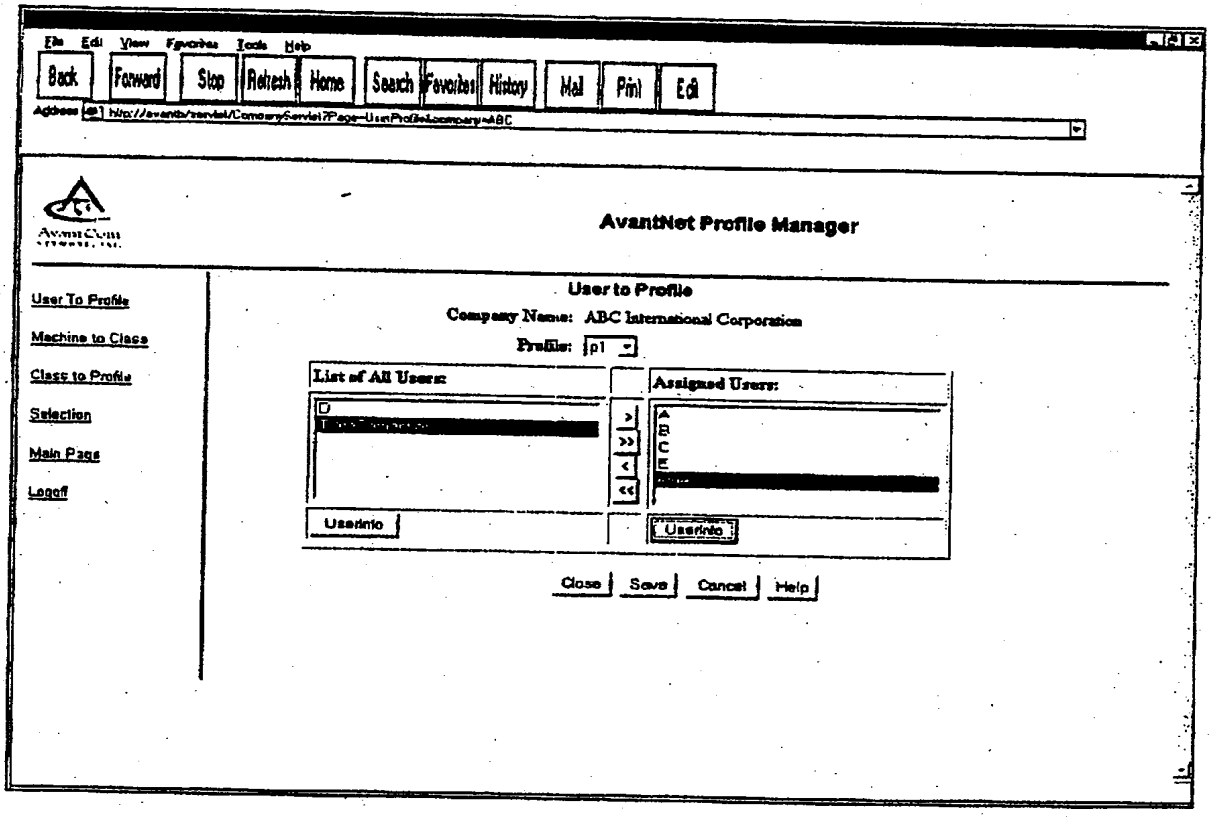

File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Address
AvantNet Profile Manager
User To Profile
Machine to Class
Class to Profile
Selection
Main Page
Logoff
User to Profile
Company Name: ABC International Corporation
Profile: p1
List of All Users:
Assigned Users:
UserInfo
UserInfo
Close
Save
Cancel
Help

FIG. 11

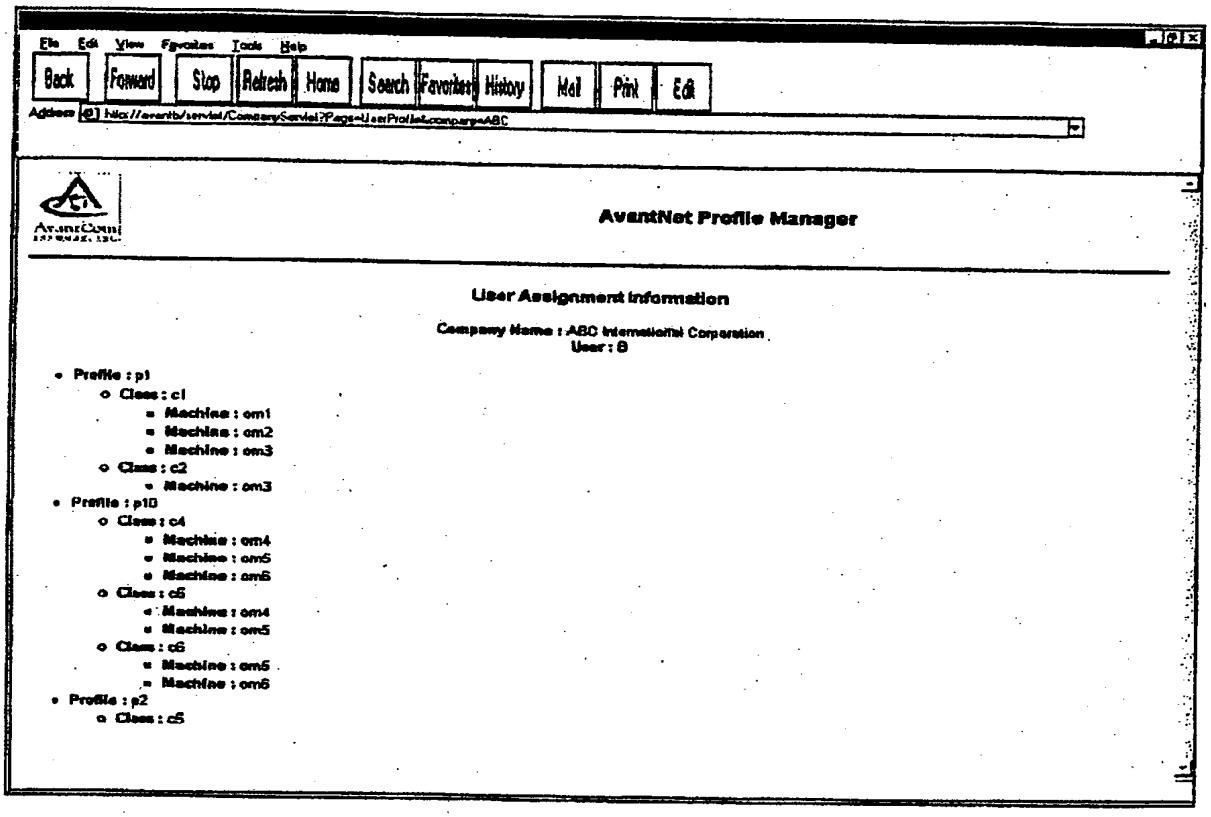


FIG. 12

BNSDOCID: <WO_____0133759A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41797

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04K 1/00; G06F 11/00, 13/36; H04L 9/32
US CL :713/173, 176, 189, 201; 709/229

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/173, 176, 189, 201; 709/229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,933,503 A (SCHELL et al.) 03 August 1999, the entire paper is relevant	1, 25, and 31
Y	US 5,864,666 A (SHRADER) 26 January 1999, the entire paper is relevant	1-39
Y	US 5,835,726 A (SHWED et al.) 10 November 1998, the entire paper is relevant	1-39
A	US 5,710,814 A (KLEMBA et al.) 20 January 1998, the entire paper is relevant	1-39
Y	US 5,606,668 A (SHWED) 25 February 1997, the entire paper is relevant	1-39

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
19 MARCH 2001	18 APR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer THOMAS BLACK
Facsimile No. (703) 305-3230	Telephone No. (703) 305-9707

Form PCT/ISA/210 (second sheet) (July 1998)★

BNSDOCID: <WO 0133759A1 | >

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41797

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,701,342 A (ANDERSON et al.) 23 December 1997, the entire paper is relevant	1-39

BNSDOCID: <WO_____0133759A1_I_>